Franchise Tax Board

SUMMARY ANALYSIS OF AMENDED BILL

Author: Jones | Analyst: Deborah Barrett | Bill Number: AB 779

Related Bills: See Prior Analysis | Telephone: 845-4301 | Amended Date: August 20, 2007

Attorney: Patrick Kusiak | Sponsor:

SUBJECT: State Agencies Notify California Resident & Office Of Privacy Protection Of Breach in Security Of Data/Required Information To Be Included In Notification

____ DEPARTMENT AMENDMENTS ACCEPTED. Amendments reflect suggestions of previous analysis of bill as introduced/amended _____.

____ AMENDMENTS IMPACT REVENUE. A new revenue estimate is provided.

____ AMENDMENTS DID NOT RESOLVE THE DEPARTMENT'S CONCERNS stated in the previous analysis of bill as introduced/amended _____.

____ FURTHER AMENDMENTS NECESSARY.

____ DEPARTMENT POSITION CHANGED TO _____.

_X_ REMAINDER OF PREVIOUS ANALYSIS OF BILL AS AMENDED July 10, 2007 STILL APPLIES.

____ OTHER – See comments below.

SUMMARY

This bill would prohibit a state agency that sells goods or services from retaining payment related data, and would require certain information be included in notices related to a breach of security issued by state agencies subject to the payment related data requirements.

SUMMARY OF AMENDMENTS

The August 20, 2007, amendments would make the following changes:

- Allow notification of a breach of security to the owner or licensee of the data to be delayed if a law enforcement agency determines the notification may impede a criminal investigation,
- Add medical information or health insurance information as data elements subject to notification requirements if unencrypted, based on double jointing language with AB 1298,
- Make the provisions of the act severable, and
- Add double jointing language to resolve chaptering issues with AB 1298.

Board Position:			Legislative Director	Date
____ S	____ NA	____ NP		
____ SA	____ O	____ NAR	Brian Putler	9/6/07
____ N	____ OUA	_X_ PENDING		

The August 20, 2007, amendments did not resolve the "Implementation Consideration" identified in the department's analysis of the bill as amended July 10, 2007, and is repeated here for convenience. The "This Bill" discussion has been revised, and the remainder of the department's analysis of the bill as amended July 10, 2007, still applies.

POSITION

Pending.

THIS BILL

This bill would prohibit, with certain exceptions, a person, business, or state agency that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device, from storing payment related data, except as specified.

This bill would also prohibit the following:

- Storage of sensitive authentication data subsequent to authorization,
- Storage of any payment related data that is not needed for business purposes,
- Retention of the primary account number unless retained in a manner consistent with other provisions of the bill and in a form that is unreadable and unusable by unauthorized persons anywhere it is stored,
- Sending payment related data across any open public network unless the data is encrypted using strong cryptography and security, and
- Allowing access to payment related data by any individual whose job does not require that access.

The provisions of this bill are not applicable to financial institutions that are in compliance with federal regulations relating to disclosure of nonpublic information if subject to compliance oversight by a state or federal regulatory agency with respect to those regulations.

This bill would require those agencies subject to the payment related data restrictions to notify the owners or licensees of the data if the system containing that data has been breached by an unauthorized person. This bill would provide that if notice is required, the agency whose system was breached is liable to the owner or licensee of the information for the reimbursement of all reasonable and actual costs of providing notice to consumers regarding the breach of the security of the system. Reasonable and actual costs include, but are not limited to, the costs of card replacement as a result of the breach of the security of the system.

This bill would require the notices to the owners or licensees of the payment related data to comply with certain requirements and specifies the type of information to be included in the notices. If the owner or licensee of the information is the issuer of the credit or debit card or the payment device, or maintains the account information from which the payment device orders payment, the owner or licensee must disclose to the California resident the information provided for in this bill.

The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and may be made after a law enforcement agency determines that the notification would not impede a criminal investigation.

This bill would provide that the owner of the personal information is entitled to reimbursement from the agency that maintained the computerized data for all reasonable and actual costs of providing notice to consumers regarding the breach of the security of the system. Reasonable and actual costs include but are not limited to the costs of card replacement as a result of the breach of the security of the system.

This bill would add medical information and health insurance information as defined, as data elements subject to notification if unencrypted and acquired by an unauthorized person. This provision is subject to double jointing language with AB 1298, which if not enacted before this bill, these additional data elements would not be applicable.

This bill would require that if substitute notice as authorized is provided, the Office of Privacy Protection must also be notified.

The provisions of this bill are intended to be severable, and the bill would repeal duplicative sections and provide double jointing language to resolve chaptering issues with AB 1298.

IMPLEMENTATION CONSIDERATIONS

Because the majority of the Franchise Tax Board's (FTB) transactions with taxpayers are payments of tax obligations, rather than purchases of goods or services, the department would interpret the bill's provisions related to the retention of payment related data to have no application to FTB. Consequently, because the July 10, 2007, amendments make the requirement to notify owners or licensees of data in the event of a security breach conditioned upon being subject to the retention of payment related data requirements, the July 10, 2007, amendments do not apply to FTB either. If it is the author's intention that these requirements apply to tax payments made to FTB, it is recommended that payments for purposes other than goods and services be expressly included.

LEGISLATIVE STAFF CONTACT

Deborah Barrett
Franchise Tax Board
(916) 845-4301
Deborah.Barrett@ftb.ca.gov

Brian Putler
Franchise Tax Board
(916) 845-6333
brian.putler@ftb.ca.gov